Chinese Remainder Theorem

Wednesday, February 9, 2022 12:46 PM

Missing:
#2, 5, 12, 22, 24
26, 32,

Recall: Linear Congruence
$a \cdot x \equiv b \pmod{n}$

1] The Chinese Remainder Theorem (CRT)

Objective: to solve a system of linear congruences (in different mod's)

Thrm: Let $m_1, m_2, \dots, m_n$ be pairwise relatively prime integers. Then the system:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 \cdot m_2 \cdot \dots \cdot m_n$

2] Proof: How to find the solution in the CRT

① let $M_k = m / m_k \implies \gcd(M_k, m_k) = 1$

② $y_k = M_k^{-1} \pmod{m_k} \implies M_k \cdot y_k \equiv 1 \pmod{m_k}$

③ then $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n \pmod{m}$

3] e.g. on CRT (by Chinese mathematician Sun-Tsu)

Solve:
$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

Sol^n.

$M_1 = 5 \cdot 7 = 35 \implies y_1 \equiv 35^{-1} \equiv 2^{-1} \equiv 2 \pmod{3}$

$M_2 = 3 \cdot 7 = 21 \implies y_2 \equiv 21^{-1} \equiv 1^{-1} \equiv 1 \pmod{5}$

$M_3 = 3 \cdot 5 = 15 \implies y_3 \equiv 15^{-1} \equiv 1^{-1} \equiv 1 \pmod{7}$

$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + \underline{2 \cdot 15 \cdot 1} \pmod{105}$

$\equiv (3+1) \cdot 35 + (5-2) \cdot 21 + (7-5) \cdot 15$

$\equiv 35 - 42 + 30 \equiv 23 \pmod{105}$

4] Computer Arithmetic with large integer: (RNS)

let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime, then by CRT, $\forall a \in \mathbb{Z}_m$, $m = \prod_i m_i$, a can be represented uniquely by the n-tuple

$$(a \bmod m_1,\ a \bmod m_2,\ \ldots,\ a \bmod m_n)$$

e.g. for $\mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$, use $m_1 = 3$, $m_2 = 4$

$0 = (0,0)$	$4 = (1,0)$	$8 = (2,0)$
$1 = (1,1)$	$5 = (2,1)$	$9 = (0,1)$
$2 = (2,2)$	$6 = (0,2)$	$10 = (1,2)$
$3 = (0,3)$	$7 = (1,3)$	$11 = (2,3)$

Add

$$\begin{array}{lcl} 6 & \longrightarrow & (0,2) \\ 5\,+ & \longrightarrow & (2,1) \\ \hline 11 & \xleftarrow{\text{CRT}} & (2,3) \end{array}$$

Mult

$$\begin{array}{lcl} 2 & \longrightarrow & (2,2) \\ 5\,\times & \longrightarrow & (2,1) \\ \hline 10 & \xleftarrow{\text{CRT}} & (1,2) \end{array}$$

5] Exer. To perform arithmetic quickly on a CPU of max-int < 100. Design an RNS for int $\lessapprox 10^6$

Sol.

let $m_1 = 99$, $m_2 = 98$, $m_3 = 97$, $m_4 = 95 \Rightarrow m = 89 \times 10^6$

$$\begin{array}{lcl} 123\,684 & \longrightarrow & (33, 8, 9, 89) \\ 413\,456\,+ & \longrightarrow & (32, 92, 2, 16) \\ \hline \boxed{\quad x \quad} & & (65, 2, 11, 10) \end{array}$$

Solve

by CRT

Solve

$$\left.\begin{aligned} x &\equiv 65 \pmod{99} \\ x &\equiv 2 \pmod{98} \\ &\vdots \\ x &\equiv 10 \pmod{95} \end{aligned}\right\}$$

by CRT

6] Hash functions :

$h(x) \longrightarrow y$ where x can be of any length and y has a fixed length

e.g.

$h(x) = x \mod 31$

the h output is of length 5 bits

e.g. $h(65) = 3 \longrightarrow (00011)_2$

7] Pseudorandom numbers

modulus m

multiplier a, $2 \leq a < m$

increment c, $0 \leq c < m$

Seed $x_0 \in \mathbb{Z}_m$

$$x_i = (a x_{i-1} + c) \mod m$$

e.g. $m = 9$, $a = 7$, $c = 4$, $x_0 = 3$

$$x_1 = 7 \cdot (3) + 4 \equiv 7 \pmod 9$$
$$x_2 = 7 \cdot 7 + 4 \equiv 8 \pmod 9$$
$$\vdots$$